Bounds for multi-end communication over quantum networks

Stefano Pirandola
Department of Computer Science, University of York, York YO10 5GH, United Kingdom and
Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA

Quantum and private communications are affected by a fundamental limitation which severely restricts the optimal rates that are achievable by two distant parties. To overcome this problem, one needs to introduce quantum repeaters and, more generally, quantum communication networks. Within a quantum network, other problems and features may appear when we move from the basic unicast setting of single-sender/single-receiver to more complex multiend scenarios, where multiple senders and multiple receivers simultaneously use the network to communicate. Assuming various configurations, including multiple-unicast, multicast, and multiple-multicast communication, we bound the optimal rates for transmitting quantum information, distributing entanglement, or generating secret keys in quantum networks connected by arbitrary quantum channels. These bounds cannot be surpassed by the most general adaptive protocols of quantum network communication.

I. INTRODUCTION

Quantum and private communications represent some of the most advanced areas of quantum information [1–5]. In particular, quantum key distribution (QKD) [6, 7] has been already developed into several commercial prototypes, besides the fact that quantum-secured networks and satellite quantum communications are being developed by various countries [8]. A more ambitious and long-term goal is that of the quantum internet [9–11] where remote quantum computers are suitable connected by optical links so as to ultimately create a worldwide architecture for distributed quantum computing.

In terms of quantum communications, one of the basic reasons to build quantum networks [12] is to overcome the rate limitations of point-to-point protocols. As shown in Ref. [13], the maximum rates at which two remote parties can transmit quantum information, distribute entanglement or secret correlations over a lossy channel of transmissivity η are all equal to $-\log_2(1-\eta)$, also known as the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound. For the specific case of QKD, this ultimate point-to-point rate can be achieved by employing a quantum memory at the sender side, as shown back in 2009 when the notion of reverse coherent information was introduced for bosonic channels [14, 15]. On the other hand, if a middle node is inserted between the remote parties, the PLOB bound can be practically beaten, as shown by the recent twin-field QKD protocol [16].

Once understood that the use of relays or repeaters [17–19] can overcome the PLOB bound, it is also important to understand the ultimate limits achievable by repeater-assisted quantum communications [20, 21]. Using techniques from network information theory [22–26] and very recent channel simulation tools developed in quantum information [13] (see also Refs. [27–32]), one can bound or exactly derive the capacities for quantum and private communication between two end-points of a repeater chain or a quantum network. This was shown in Ref. [20] which reports the end-to-end (unicast) results originally established in the 2016 unpublished work [21].

The present paper reports and refines the other (multi-end) results of unpublished [21], thus providing a generalization of Ref. [20] from the unicast setting of single-sender/single-receiver to more complex scenarios where multiple senders and receivers are involved. In these scenarios, the remote parties compete with the others in order to make an optimal use of the quantum network. We assume different configurations, including multiple-unicast (where there are many single-sender/single-receiver pairs trying to communicate in a simultaneous fashion), multicast (where a single-sender tries to communicate with multiple receivers), and multiple-multicast (where different senders try to communicate with the same set of multiple receivers). In all these communication configurations, we derive single-letter upper bounds for the maximum rates at which the parties can transmit quantum information, distribute entanglement or secret keys. These bounds are valid for networks connected by arbitrary quantum channels and are expressed in terms of the relative entropy of entanglement (REE) [33–35].

It is important to remark that the results apply to both discrete- and continuous-variable systems, i.e., quantum networks connected by quantum channels acting over finite- or infinite-dimensional spaces. In fact, as discussed afterwards, the theory presented for finite dimension d can be extended to $d=+\infty$ by generalizing the notion of channel simulation to an asymptotic formulation which is based on a sequence of finite-energy resource states. Thanks to this tool, we can compute the relevant functionals on the sequence and then take the infinite-energy limit of their values over the sequence. In this way, we automatically and rigorously prove the results for bosonic channels, following the methods that were originally designed in Refs. [13, 20, 21].

The paper is organized as follows. In Sec. II we present preliminary notions on adaptive protocols, besides the tools of simulation and stretching for channels [13] and networks [20]. The expert reader can skip this part and directly start from Sec. III which provides general description of the various configurations considered in this work. Secs. IV and V consider multiple-unicast settings under single- and multi-path routing strategies for the

quantum systems. Sec. VI investigates the case of multicast communication from a sender to multiple receivers. Following Sec. VII considers multiple-multicast communication between many senders and many receivers. Finally, Sec. VIII is for conclusions.

II. PRELIMINARIES

A. Adaptive point-to-point protocols

Let us first discuss the general structure of an adaptive point-to-point protocol $\mathcal{P}$ through a quantum channel $\mathcal{E}$, following the notation from Ref. [13]. Alice has a local register of quantum systems $\mathbf{a}$ and Bob has another local register $\mathbf{b}$; these are prepared in a state $\rho^0_{\mathbf{ab}}$ by means of local operations (LOs) assisted by two-way classical communication (CC), also known as adaptive LOCCs. After the first adaptive LOCC Λ_0, Alice selects a system $a_1 \in \mathbf{a}$ and sends it to Bob through the quantum channel $\mathcal{E}$. Once Bob receives the output b_1, this is included in his register $b_1\mathbf{b} \to \mathbf{b}$ and another adaptive LOCC Λ_1 is performed by the parties. The second transmission starts by selecting another system $a_2 \in \mathbf{a}$ which is sent through $\mathcal{E}$ whose output a_2 is received by Bob. Bob updates his register $b_2\mathbf{b} \to \mathbf{b}$ and another adaptive LOCC Λ_2 is performed. The generic i-th transmission is shown in Fig. 1. After n uses, Alice and Bob have implemented an adaptive protocol $\mathcal{P}$ defined by the sequence of LOCCs $\{\Lambda_0, \Lambda_1 \ldots\}$ and providing an output state $\rho^n_{\mathbf{ab}}$ close in trace norm to a target state ϕ^n with nR^ε_n (target) bits, i.e., such that $\|\rho^n_{\mathbf{ab}} - \phi^n\| \leq \varepsilon$.

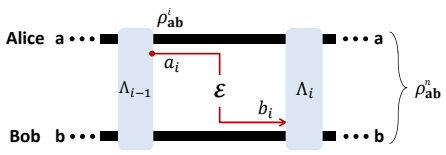

FIG. 1: Generic ith transmission through channel $\mathcal{E}$ in a point-to-point adaptive protocol. The transmission $a_i \to b_i$ is interleaved by two adaptive LOCCs, Λ_{i-1} and Λ_i, performed by Alice and Bob on their local registers $\mathbf{a}$ and $\mathbf{b}$.

If we now consider the limit for large n (asymptotic rate) and small ε (weak converse), and then we optimize over the protocols $\mathcal{P}$, we define the two-way assisted capacity of $\mathcal{E}$, i.e.,

$$\mathcal{C}(\mathcal{E}) := \sup_{\mathcal{P}} \lim_{\varepsilon,n} R^\varepsilon_n. \tag{1}$$

Assume that the target ϕ^n is a maximally-entangled state, so that the target bits are entanglement bits (ebits). In this case, $\mathcal{C}(\mathcal{E})$ corresponds to the two-way entanglement-distribution capacity $D_2(\mathcal{E})$, which is also equal to the two-way quantum capacity $Q_2(\mathcal{E})$. Assume instead that ϕ^n is a private state [36], so that the target bits are private bits, then $\mathcal{C}(\mathcal{E})$ corresponds to the secret key capacity $K(\mathcal{E}) \geq D_2(\mathcal{E})$.

B. LOCC simulation of quantum channels

One may follow the general recipe of Ref. [13] to simplify an adaptive protocol over $\mathcal{E}$ and write a single-letter upper bound for the two-way assisted capacity $\mathcal{C}(\mathcal{E})$. The first step is the simulation of the channel $\mathcal{E}$ by means of an LOCC $\mathcal{T}$ and some resource state σ. For any channel $\mathcal{E}$, we may always find a simulation such that

$$\mathcal{E}(\rho) = \mathcal{T}(\rho \otimes \sigma). \tag{2}$$

A channel simulable with resource state σ may also be called "σ-stretchable". It is important to note that the simulation may also be asymptotic, so that we have a sequence of LOCCs $\mathcal{T}^\mu$ and resource states σ^μ such that we may write the point-wise limit [13]

$$\mathcal{E}(\rho) = \lim_\mu \mathcal{T}^\mu(\rho \otimes \sigma^\mu). \tag{3}$$

A very convenient simulation holds for those channels commuting with the teleportation correction unitaries, which are (generalized) Pauli operators in finite dimension and phase-space displacements in continuous variable systems [40]. By definition, a quantum channel $\mathcal{E}$ is called teleportation-covariant, or just "telecovariant" when, for any teleportation unitary U, we may write

$$\mathcal{E}(U\rho U^\dagger) = V\mathcal{E}(\rho)V^\dagger \ , \tag{4}$$

for another (generally-different) unitary V. Note that Pauli channels [1], erasure channels and bosonic Gaussian channels [4] are all telecovariant.

For a telecovariant channel $\mathcal{E}$, we write the simulation

$$\mathcal{E}(\rho) = \mathcal{T}_{\text{tele}}(\rho \otimes \sigma_{\mathcal{E}}), \tag{5}$$

where $\mathcal{T}_{\text{tele}}$ is a teleportation protocol [37–40] and $\sigma_{\mathcal{E}} := \mathcal{I} \otimes \mathcal{E}(\Phi)$ is the Choi matrix of the channel, with Φ being a maximally entangled state. For bosonic Gaussian channels, the Choi matrix is asymptotic, i.e., defined by the μ-limit of the sequence $\sigma^\mu_{\mathcal{E}} := \mathcal{I} \otimes \mathcal{E}(\Phi^\mu)$, where Φ^μ is a two-mode squeezed vacuum (TMSV) state with variance parameter μ [4]. Thus, we may write the asymptotic simulation

$$\mathcal{E}(\rho) = \lim_\mu \mathcal{T}^\mu_{\text{tele}}(\rho \otimes \sigma^\mu_{\mathcal{E}}), \tag{6}$$

where $\mathcal{T}^\mu_{\text{tele}}$ is a sequence of teleportation-LOCCs.

C. Stretching and single-letter bound

In an adaptive protocol, we may replace each transmission through the channel $\mathcal{E}$ with its simulation $(\mathcal{T}, \sigma)$. Then, as shown in Ref. [13], we may collapse all the simulation LOCCs $\mathcal{T}$ and the adaptive LOCCs of the protocol $\{\Lambda_0, \Lambda_1 \ldots\}$ into a single trace-preserving LOCC $\bar{\Lambda}$. In this way, the n-use output state of the protocol can be decomposed as

$$\rho^n_{\mathbf{ab}} = \bar{\Lambda}\left(\sigma^{\otimes n}\right). \tag{7}$$

If the simulation of the channel is asymptotic, the stretching takes the form $\rho^n_{\mathbf{ab}} = \lim_\mu \bar{\Lambda}_\mu(\sigma^{\mu\otimes n})$ for a sequence of trace-preserving LOCC $\bar{\Lambda}_\mu$ and resource states σ^μ. See Ref. [13, 29, 30] for a precise formulation of this limit where the simulation error is explicitly taken into account.

Suppose that we want to compute an entanglement measure over the output state. In particular, let us consider the REE. For a quantum state ρ, this is [33]

$$E_{\mathrm{R}}(\rho) = \inf_{\gamma\in\mathrm{SEP}} S(\rho||\gamma), \tag{8}$$

where γ is an arbitrary separable state and S is the quantum relative entropy $S(\rho||\gamma) := \mathrm{Tr}\left[\rho(\log_2\rho - \log_2\gamma)\right]$. More weakly, if we consider an asymptotic state $\sigma := \lim_\mu \sigma^\mu$, the previous definition can be extended as

$$E_{\mathrm{R}}(\sigma) = \liminf_{\mu\to+\infty} E_{\mathrm{R}}(\sigma^\mu) = \inf_{\gamma^\mu} \liminf_{\mu\to+\infty} S(\sigma^\mu||\gamma^\mu), \tag{9}$$

where γ^μ is a converging sequence of separable states [13].

Because the REE is monotonic under trace-preserving LOCCs (data processing) and sub-additive over tensor products, we may write

$$E_{\mathrm{R}}(\rho^n_{\mathbf{ab}}) = E_{\mathrm{R}}\left[\bar{\Lambda}\left(\sigma^{\otimes n}\right)\right] \leq E_{\mathrm{R}}\left(\sigma^{\otimes n}\right) \leq nE_{\mathrm{R}}\left(\sigma\right). \tag{10}$$

Now recall that the REE is also asymptotically continuous. This means that for $\rho^n_{\mathbf{ab}}$ and ϕ^n such that $\|\rho^n_{\mathbf{ab}} - \phi^n\| \leq \varepsilon$, we may write

$$|E_{\mathrm{R}}(\phi^n) - E_{\mathrm{R}}(\rho^n_{\mathbf{ab}})| \leq \delta(d,\varepsilon), \tag{11}$$

where $\delta(\varepsilon, d)$ depends the ε-closeness, and the dimension d of the total Hilbert space. In the limit of large n and small ε (weak converse), we can neglect $\delta(\varepsilon,d)/n$. This is a straightforward application of the exponential scaling of the dimension d shown in Refs. [41, 42] for DV systems and extended to CV systems in Ref. [13]. For a simplified treatment for CV systems see also Ref. [29]. Because $E_{\mathrm{R}}(\phi^n) \geq nR^\varepsilon_n$ [36], we therefore have

$$R^\varepsilon_n \leq E_{\mathrm{R}}\left(\sigma\right) + n^{-1}\delta(d,\varepsilon), \tag{12}$$

which leads to the single-letter upper bound [13]

$$\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}(\sigma). \tag{13}$$

In particular, for telecovariant $\mathcal{E}$, we may write

$$\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}(\sigma_{\mathcal{E}}), \tag{14}$$

with a suitable asymptotic formulation for bosonic Gaussian channels based on Eq. (9).

Among telecovariant channels, the "distillable" ones are those for which we may write $E_{\mathrm{R}}(\sigma_{\mathcal{E}}) = D_1(\sigma_{\mathcal{E}})$, where $D_1(\sigma_{\mathcal{E}})$ is the distillable entanglement of the (possibly-asymptotic) channel's Choi matrix $\sigma_{\mathcal{E}}$ via one-way CCs, forward or backward. This is lower-bounded by both the coherent [43, 44] and reverse coherent [14, 15] information of the Choi matrix. For a distillable channel, the two-way capacities coincide and are given by

$$\mathcal{C}(\mathcal{E}) = E_{\mathrm{R}}(\sigma_{\mathcal{E}}) = D_1(\sigma_{\mathcal{E}}). \tag{15}$$

This is the case for a number of channels, including the dephasing channel, the erasure channel, the pure-loss channel and the quantum-limited amplifier. For a pure-loss channel with transmissivity η, the two-way capacity is simply given by the PLOB bound [13, Eq. (19)]

$$\mathcal{C}(\eta) = -\log_2(1-\eta)\ . \tag{16}$$

As secret-key capacity, this bounds the maximum rate of any point-to-point QKD protocol.

D. Notation for quantum networks

We model a quantum communication network $\mathcal{N}$ as an undirected finite graph [22] $\mathcal{N} = (P, E)$, where P is the set of points or nodes, and E is the set of undirected edges. Every point can be identified with a corresponding local register $\mathbf{p}$ of quantum systems. The existence of an edge $(\mathbf{x},\mathbf{y})$, between two points $\mathbf{x}$ and $\mathbf{y}$, means that there is a physical quantum channel $\mathcal{E}_{\mathbf{xy}}$ between them (which can be forward $\mathcal{E}_{\mathbf{x}\to\mathbf{y}}$ or backward $\mathcal{E}_{\mathbf{y}\to\mathbf{x}}$). For points $\mathbf{p}_i$ and $\mathbf{p}_j$, we also use the short-hand notation $\mathcal{E}_{ij} := \mathcal{E}_{\mathbf{p}_i\mathbf{p}_j}$. We use the notation $\mathbf{a}$ and $\mathbf{b}$ for Alice and Bob, respectively. A path or route between these two end-points is a sequence of edges $(\mathbf{a},\mathbf{p}_i),\cdots,(\mathbf{p}_j,\mathbf{b})$, that we may simply denote as $\mathbf{a}-\mathbf{p}_i-\cdots-\mathbf{p}_j-\mathbf{b}$. For a route with N middle points (or repeaters), we have $N+1$ edges and, therefore, a corresponding sequence of $N+1$ channels $\{\mathcal{E}_0,\cdots,\mathcal{E}_k,\cdots,\mathcal{E}_N\}$ from Alice to Bob.

There are different possible routes between two end-points. For this reason, they may also use different routing strategies. In single-path routing, Alice and Bob exploit a single route in each use of the network, and this route can be changed for the different network uses. In multi-path routing, Alice and Bob exploit many routes in parallel in each use of the network. In particular, they may adopt a flooding strategy [45] where each edge of the network is used exactly once in each end-to-end transmission. In both cases, we assume that the quantum protocols are adaptive, meaning that each transmission through each channel is interleaved with a network adaptive LOCCs, where all points of the network apply LOs on their local registers assisted by unlimited two-way CC with all the other points of the network.

An entanglement cut C of the quantum network $\mathcal{N}$ is a bipartition $(\mathbf{A},\mathbf{B})$ of all the points P such that $\mathbf{a}\in\mathbf{A}$ and $\mathbf{b}\in\mathbf{B}$. Correspondingly, the cut-set $\tilde{C}$ of C is the ensemble of edges across the bipartition, i.e., $\tilde{C} = \{(\mathbf{x},\mathbf{y})\in E : \mathbf{x}\in\mathbf{A}, \mathbf{y}\in\mathbf{B}\}$. It is clear that $\tilde{C}$ also identifies an ensemble of channels $\{\mathcal{E}_{\mathbf{xy}}\}_{(\mathbf{x},\mathbf{y})\in\tilde{C}}$. Given a cut, we may also consider the complementary sets

$$\tilde{A} = \{(\mathbf{x},\mathbf{y})\in E : \mathbf{x},\mathbf{y}\in\mathbf{A}\}, \tag{17}$$

$$\tilde{B} = \{(\mathbf{x},\mathbf{y})\in E : \mathbf{x},\mathbf{y}\in\mathbf{B}\}, \tag{18}$$

so that $\tilde{A} \cup \tilde{B} \cup \tilde{C} = E$.

Given an undirected network $\mathcal{N} = (P, E)$ we can introduce an orientation by transforming it in a directed graph. One can choose a direction for all edges so that a generic edge $(\mathbf{x}, \mathbf{y})$ becomes an ordered pair where $\mathbf{x}$ is the "tail" and $\mathbf{y}$ is the "head". In choosing these directions, we keep Alice as tail and Bob as head, so that the quantum network can be represented as a flow network where Alice is the *source* and Bob is the *sink* [46–50]. There are $\mathcal{O}(2^{|E|})$ possible orientations. Given an orientation of $\mathcal{N}$, there is a corresponding flow network $\mathcal{N}_D = (P, E_D)$, where E_D is the set of directed edges. Then, for arbitrary point $\mathbf{p}$, we define its out-neighborhood as the set of heads going from $\mathbf{p}$

$$N^{\text{out}}(\mathbf{p}) = \{\mathbf{x} \in P : (\mathbf{p}, \mathbf{x}) \in E_D\}, \tag{19}$$

and its in-neighborhood as the set of tails going into $\mathbf{p}$

$$N^{\text{in}}(\mathbf{p}) = \{\mathbf{x} \in P : (\mathbf{x}, \mathbf{p}) \in E_D\}. \tag{20}$$

A multi-message quantum multicast from point $\mathbf{p}$ is a point-to-multipoint connection from $\mathbf{p}$ to part of its out-neighborhood $N^{\text{out}}(\mathbf{p})$, so that different messages (quantum states or keys) are received by the receiving points. It is a single-message multicast if the messages coincide.

E. Simulation and stretching of a network

Given an arbitrary network $\mathcal{N}$, we may replace it with its simulation [20, 21]. In fact, for any edge $(\mathbf{x}, \mathbf{y})$, we may replace the quantum channel $\mathcal{E}_{\mathbf{xy}}$ with its simulation $S_{\mathbf{xy}} = (\mathcal{T}_{\mathbf{xy}}, \sigma_{\mathbf{xy}})$ for some LOCC $\mathcal{T}_{\mathbf{xy}}$ and resource state $\sigma_{\mathbf{xy}}$. Repeating this process for all the edges defines an LOCC simulation of the network $S(\mathcal{N}) = \{S_{\mathbf{xy}}\}_{(\mathbf{x},\mathbf{y})\in E}$ where all channels $\mathcal{E}_{\mathbf{xy}}$ are replaced by resource states $\sigma_{\mathbf{xy}}$. There is a corresponding resource representation of the network $\sigma(\mathcal{N}) = \{\sigma_{\mathbf{xy}}\}_{(\mathbf{x},\mathbf{y})\in E}$. See also Fig. 2 for a simple example. In particular, for a telecovariant network, where all channels are telecovariant, then the simulation involves teleportation LOCCs and the network can be replaced by its Choi representation $\sigma(\mathcal{N}) = \{\sigma_{\mathcal{E}_{\mathbf{xy}}}\}_{(\mathbf{x},\mathbf{y})\in E}$. Here each channel $\mathcal{E}_{\mathbf{xy}}$ is replaced by its (possibly-asymptotic) Choi matrix $\sigma_{\mathcal{E}_{\mathbf{xy}}}$. A quantum network is said to be distillable if it is connected by distillable channels.

Given an arbitrary adaptive protocol implemented over the quantum network $\mathcal{N}$, we can use the network simulation $\sigma(\mathcal{N})$ to stretch the protocol and decompose the total output state $\rho^n_{\mathbf{a}\ldots\mathbf{b}}$ of network after n uses as follows

$$\rho^n_{\mathbf{a}\ldots\mathbf{b}} = \bar{\Lambda}\left[\bigotimes_{(\mathbf{x},\mathbf{y})\in E} \sigma_{\mathbf{xy}}^{\otimes n_{\mathbf{xy}}}\right], \tag{21}$$

where $\bar{\Lambda}$ is a trace-preserving LOCC and $n_{\mathbf{xy}}$ is the number of uses of the edge $(\mathbf{x}, \mathbf{y})$. In particular, we have $n_{\mathbf{xy}} \leq n$ ($n_{\mathbf{xy}} = n$) for a single-path (flooding) protocol. In other words, introducing the probabilities $p_{\mathbf{xy}} := n_{\mathbf{xy}}/n$ we have $p_{\mathbf{xy}} \leq 1$ ($= 1$) for a single-path (flooding) protocol [20, 21].

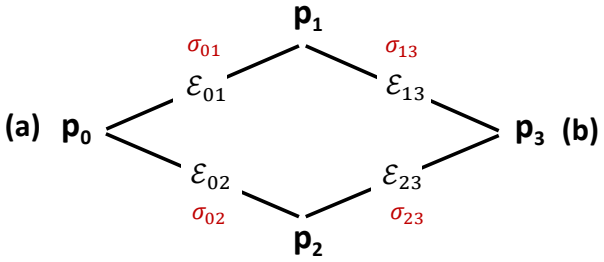

FIG. 2: Network simulation. Consider a simple four-point quantum network $\mathcal{N} = (\{\mathbf{p}_0, \mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3\}, E)$ with end points $\mathbf{p}_0 = \mathbf{a}$ (Alice) $\mathbf{p}_3 = \mathbf{b}$ (Bob). Edge $(\mathbf{p}_i, \mathbf{p}_j)$ has an associated quantum channel $\mathcal{E}_{ij}$. By simulating each channel $\mathcal{E}_{ij}$ with a corresponding resource state σ_{ij}, we define a resource representation of the network $\sigma(\mathcal{N}) = \{\sigma_{01}, \sigma_{02}, \sigma_{13}, \sigma_{23}\}$.

Tracing out all the network points except the two end-points, from Eq. (21) we get Alice and Bob's shared state $\rho^n_{\mathbf{ab}}$. For any entanglement cut C and corresponding cut-set $\tilde{C}$, we may write a better decomposition for Alice and Bob's output state. This is given by

$$\rho^n_{\mathbf{ab}}(C) = \bar{\Lambda}_{\mathbf{ab}}\left[\bigotimes_{(\mathbf{x},\mathbf{y})\in\tilde{C}} \sigma_{\mathbf{xy}}^{\otimes n_{\mathbf{xy}}}\right], \tag{22}$$

where $\bar{\Lambda}_{\mathbf{ab}}$ is a trace-preserving LOCC with respect to Alice and Bob. Previous Eqs. (21) and (22) can be extended to asymptotic resource states by introducing suitable limits. See Ref. [20, 21] for more details on these methods.

III. MULTIPLE SENDERS AND RECEIVERS

One of the basic working mechanisms in a quantum communication network is the unicast setting, based on a single sender $\mathbf{a}$ and a single receiver $\mathbf{b}$. However, in general, we may consider multiple senders $\{\mathbf{a}_i\}$ and receivers $\{\mathbf{b}_j\}$, which may simultaneously communicate according to various configurations. For simplicity, these sets are intended to be disjoint $\{\mathbf{a}_i\} \cap \{\mathbf{b}_j\} = \emptyset$, so that an end-point cannot be sender and receiver at the same time. It is clear that all the results from Ref. [20, 21], derived for the two basic routing strategies, provide general upper bounds which are still valid for the individual end-to-end capacities associated with each sender-receiver pair $(\mathbf{a}_i, \mathbf{b}_i)$ in the various settings with multiple end-points.

In the following sections, we start with the multiple-unicast quantum network. This consists of M Alices $\{\mathbf{a}_1, \ldots, \mathbf{a}_M\}$ and M Bobs $\{\mathbf{b}_1, \ldots, \mathbf{b}_M\}$, with the generic ith Alice $\mathbf{a}_i$ communicating with a corresponding ith Bob $\mathbf{b}_i$. This case can be studied by assuming single-path routing (Sec. IV) or multipath routing (Sec. V). Besides the general bounds inherited from the unicast

scenario, we derive a specific set of upper bounds for the rates that are simultaneously achievable by all parties.

Another important case is the multicast (multi-message) quantum network, where a single sender simultaneously communicates with $M \geq 1$ receivers, e.g., for distributing M different states or keys. By its nature, this is studied under multipath routing (Sec. VI). In this setting, an interesting variant is the distribution of the same key to all receivers (single-message multicast).

More generally, we may consider a multiple-multicast (multi-message) quantum network. Here we have $M_A \geq 1$ senders and $M_B \geq 1$ receivers, and each sender communicates simultaneously with the entire set of receivers communicating different states or keys (Sec. VII). In a private communication scenario, this corresponds to the distribution of $M_A M_B$ different keys. For a description of these configurations, see the simple example of the butterfly quantum network in Fig. 3.

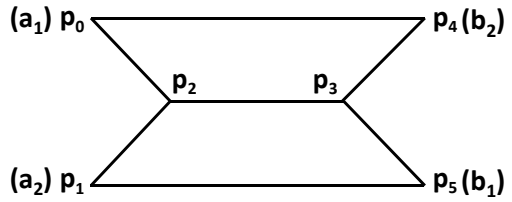

FIG. 3: Butterfly quantum network. (i) An example of multiple-unicast is considering two sender-receiver pairs, e.g., Alice $\mathbf{a}_1$ communicating with Bob $\mathbf{b}_1$, and Alice $\mathbf{a}_2$ with Bob $\mathbf{b}_2$. Single-path routing corresponds to the simultaneous use of two end-to-end routes, e.g., $(\mathbf{a}_1)\mathbf{p}_0-\mathbf{p}_2-\mathbf{p}_3-\mathbf{p}_5(\mathbf{b}_1)$ and $(\mathbf{a}_2)\mathbf{p}_1-\mathbf{p}_2-\mathbf{p}_3-\mathbf{p}_4(\mathbf{b}_2)$. Multipath routing corresponds to choosing a network orientation, where the end-points may also act as relays. Each point of the network multicasts multiple messages to its out-neighborhood. For instance, we may have the point-to-multipoint multicasts: $\mathbf{p}_0 \to \{\mathbf{p}_2, \mathbf{p}_4\}$, $\mathbf{p}_1 \to \{\mathbf{p}_2, \mathbf{p}_5\}$, $\mathbf{p}_2 \to \mathbf{p}_3$, and $\mathbf{p}_3 \to \{\mathbf{p}_4, \mathbf{p}_5\}$. (ii) An example of network multicast is Alice $\mathbf{a}_1$ communicating with the two Bobs $\{\mathbf{b}_1, \mathbf{b}_2\}$ via multipath routing. In general, the messages (states, keys) can be different. (iii) In a multiple-multicast, Alice $\mathbf{a}_1$ communicates with $\{\mathbf{b}_1, \mathbf{b}_2\}$, and Alice $\mathbf{a}_2$ communicates with the same destination set $\{\mathbf{b}_1, \mathbf{b}_2\}$. In general, the messages (states, keys) can be different.

IV. MULTIPLE-UNICAST QUANTUM NETWORKS WITH SINGLE-PATH ROUTING

Let us start by considering two Alice-Bob pairs $(\mathbf{a}_1, \mathbf{b}_1)$ and $(\mathbf{a}_2, \mathbf{b}_2)$, since the extension to arbitrary number of pairs is immediate. We may easily formulate network protocols which are based on single-path routing. In this case, each sequential use of the network involves the transmission of quantum systems along two (potentially-overlapping) routes

$$\omega_1 : \mathbf{a}_1 - \cdots - \mathbf{b}_1, \quad \omega_2 : \mathbf{a}_2 - \cdots - \mathbf{b}_2, \tag{23}$$

where each transmission through an edge is assisted by network LOCCs. The routes are updated use after use.

After n uses, the output of the double-unicast network protocol $\mathcal{P}_{2\text{-unicast}}$ is a state $\rho^n_{\mathbf{a}_1\mathbf{a}_2\mathbf{b}_1\mathbf{b}_2}$ which is ε-close in trace norm to a target state

$$\phi := \phi_{\mathbf{a}_1\mathbf{b}_1}^{\otimes nR_1^{\varepsilon,n}} \otimes \phi_{\mathbf{a}_2\mathbf{b}_2}^{\otimes nR_2^{\varepsilon,n}}, \tag{24}$$

where $\phi_{\mathbf{a}_i\mathbf{b}_i}$ is a one-bit state (private bit or ebit) for the pair $(\mathbf{a}_i, \mathbf{b}_i)$ and $nR_i^{\varepsilon,n}$ the number of its copies. Taking the limit of large n, small ε (weak converse) and optimizing over all protocols $\mathcal{P}_{2\text{-unicast}}$, we define the capacity region as the closure of the set of the achievable asymptotic rates (R_1, R_2). In general, for M sender-receiver pairs, we have an M-tuple of achievable rates $(R_1, \ldots, R_M)$. Depending on the task of the protocol (i.e., the target state), these rates refer to end-to-end entanglement distillation (equivalently, error-free quantum communication) or secret-key generation.

Before proceeding, let us first introduce more general types of entanglement cuts of the quantum network. Given two sets of senders $\{\mathbf{a}_i\}$ and receivers $\{\mathbf{b}_i\}$, we adopt the notation $C : \{\mathbf{a}_i\}|\{\mathbf{b}_i\}$ for a cut $C = (\mathbf{A}, \mathbf{B})$ such that $\{\mathbf{a}_i\} \subset \mathbf{A}$ and $\{\mathbf{b}_i\} \subset \mathbf{B}$. Similarly, we write $C : \mathbf{a}_i|\mathbf{b}_i$ for a cut with $\mathbf{a}_i \in \mathbf{A}$ and $\mathbf{b}_i \in \mathbf{B}$, and $C : \mathbf{a}_i\mathbf{a}_j|\mathbf{b}_i\mathbf{b}_j$ for a cut with $\{\mathbf{a}_i, \mathbf{a}_j\} \subset \mathbf{A}$ and $\{\mathbf{b}_i, \mathbf{b}_j\} \subset \mathbf{B}$. Define also the single-edge flow of entanglement (REE) trough a cut as

$$E_{\mathrm{R}}(C) := \max_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_R(\sigma_{\mathbf{xy}}), \tag{25}$$

where $\sigma_{\mathbf{xy}}$ is a resource state associated with an edge $(\mathbf{x}, \mathbf{y})$ in the cut-set $\tilde{C}$, under some simulation of the network. We can then state the following result.

Theorem 1 (Multi-unicast with single paths) *Let us consider a multiple-unicast quantum network $\mathcal{N} = (P, E)$ with M sender-receiver pairs $(\mathbf{a}_i, \mathbf{b}_i)$ communicating by means of single-path routing. Adopt a simulation of the network with a resource representation $\sigma(\mathcal{N}) = \{\sigma_{\mathbf{xy}}\}_{(\mathbf{x},\mathbf{y})\in E}$. In particular, $\sigma(\mathcal{N})$ can be a Choi-representation for a teleportation-covariant $\mathcal{N}$. We have the following outer bounds for the capacity region*

$$R_i \leq \min_{C:\mathbf{a}_i|\mathbf{b}_i} E_{\mathrm{R}}(C) \quad \textit{for any } i, \tag{26}$$

$$R_i + R_j \leq \min_{C:\mathbf{a}_i\mathbf{a}_j|\mathbf{b}_i\mathbf{b}_j} E_{\mathrm{R}}(C) \quad \textit{for any } i \neq j \tag{27}$$

$$\vdots$$

$$\sum_{i=1}^{M} R_i \leq \min_{C:\{\mathbf{a}_i\}|\{\mathbf{b}_i\}} E_{\mathrm{R}}(C), \tag{28}$$

where $E_{\mathrm{R}}(C)$ is the single-edge flow of REE through cut C. It is understood that formulations may be asymptotic for quantum networks with bosonic channels.

Proof. For simplicity, first consider the case $M = 2$, since the generalization to arbitrary M is straightforward. Let us also consider key generation, since it automatically provides an upper bound for all the other

tasks. Considering the bipartition $\mathbf{a}_1\mathbf{a}_2|\mathbf{b}_1\mathbf{b}_2$, the distillable key of the target state ϕ in Eq. (24) is equal to

$$K_{\rm D}(\mathbf{a}_1\mathbf{a}_2|\mathbf{b}_1\mathbf{b}_2)_{\phi}=n(R_1^{\varepsilon,n}+R_2^{\varepsilon,n}). \tag{29}$$

Using the REE with respect to the same bipartition, we may write the upper bound

$$\begin{aligned} n(R_1^{\varepsilon,n}+R_2^{\varepsilon,n}) &\leq E_{\rm R}(\mathbf{a}_1\mathbf{a}_2|\mathbf{b}_1\mathbf{b}_2)_{\phi} \\ &\leq E_{\rm R}(\mathbf{a}_1\mathbf{a}_2|\mathbf{b}_1\mathbf{b}_2)_{\rho^n}+\delta(\varepsilon,d), \end{aligned} \tag{30}$$

where the latter inequality comes from the fact that $\rho^n:=\rho^n_{\mathbf{a}_1\mathbf{a}_2\mathbf{b}_1\mathbf{b}_2}$ is ε-close to ϕ. The extra term $\delta(\varepsilon,d)$ depends on the ε-closeness and the dimension d of the total Hilbert space, as already discussed in relation to Eq. (11). The term $n^{-1}\delta(d,\varepsilon)$ goes to zero for large n and small ε. As a result we may write

$$\lim_{\varepsilon,n}(R_1^{\varepsilon,n}+R_2^{\varepsilon,n})\leq \lim_{n\to+\infty} n^{-1}E_{\rm R}(\mathbf{a}_1\mathbf{a}_2|\mathbf{b}_1\mathbf{b}_2)_{\rho^n}\ . \tag{31}$$

By simulating and stretching the network, we may write the following decomposition of the output state

$$\rho^n_{\mathbf{a}_1\mathbf{a}_2\mathbf{b}_1\mathbf{b}_2}=\bar{\Lambda}_{\mathbf{a}_1\mathbf{a}_2\mathbf{b}_1\mathbf{b}_2}\left[\bigotimes_{(\mathbf{x},\mathbf{y})\in E}\sigma_{\mathbf{xy}}^{\otimes n_{\mathbf{xy}}}\right], \tag{32}$$

where $n_{\mathbf{xy}}=np_{\mathbf{xy}}$ is the number of uses of edge $(\mathbf{x},\mathbf{y})$ and $\bar{\Lambda}_{\mathbf{a}_1\mathbf{a}_2\mathbf{b}_1\mathbf{b}_2}$ is a trace-preserving LOCC, which is local with respect to the bipartition $\mathbf{a}_1\mathbf{a}_2|\mathbf{b}_1\mathbf{b}_2$. By inserting entanglement cuts which disconnect the senders and receivers, we reduce the number of resource states appearing in Eq. (32) while preserving the locality of the LOCC with respect to the bipartition of the end-points. In other words, for any cut $C:\mathbf{a}_1\mathbf{a}_2|\mathbf{b}_1\mathbf{b}_2$ we may write

$$\rho^n_{\mathbf{a}_1\mathbf{a}_2\mathbf{b}_1\mathbf{b}_2}(C)=\bar{\Lambda}^C_{\mathbf{a}_1\mathbf{a}_2\mathbf{b}_1\mathbf{b}_2}\left[\bigotimes_{(\mathbf{x},\mathbf{y})\in\tilde{C}}\sigma_{\mathbf{xy}}^{\otimes n_{\mathbf{xy}}}\right]. \tag{33}$$

Using the latter decomposition in Eq. (31), we obtain

$$\begin{aligned} \lim_{\varepsilon,n}(R_1^{\varepsilon,n}+R_2^{\varepsilon,n}) &\leq \lim_{n\to+\infty} n^{-1}E_{\rm R}(\mathbf{a}_1\mathbf{a}_2|\mathbf{b}_1\mathbf{b}_2)_{\rho^n(C)} \\ &\leq \lim_{n\to+\infty} n^{-1}\sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} n_{\mathbf{xy}}E_{\rm R}(\sigma_{\mathbf{xy}}) \\ &= \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} p_{\mathbf{xy}}E_{\rm R}(\sigma_{\mathbf{xy}}) \\ &\leq \max_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\rm R}(\sigma_{\mathbf{xy}}):=E_{\rm R}(C). \end{aligned} \tag{34}$$

By minimizing over the cuts, we derive

$$\lim_{\varepsilon,n}(R_1^{\varepsilon,n}+R_2^{\varepsilon,n})\leq \min_{C:\mathbf{a}_1\mathbf{a}_2|\mathbf{b}_1\mathbf{b}_2} E_{\rm R}(C). \tag{35}$$

It is important to note that this bound holds for any protocol $\mathcal{P}_{\text{2-unicast}}$, whose details are all collapsed in the LOCC $\bar{\Lambda}_{\mathbf{a}_1\mathbf{a}_2\mathbf{b}_1\mathbf{b}_2}$ and therefore discarded. Thus, the same bound applies if we optimize over all protocols, which means that Eq. (35) provides the following outer bound for the capacity region

$$\begin{aligned} R_1+R_2 &= \sup_{\mathcal{P}_{\text{2-unicast}}}\lim_{\varepsilon,n}(R_1^{\varepsilon,n}+R_2^{\varepsilon,n}) \\ &\leq \min_{C:\mathbf{a}_1\mathbf{a}_2|\mathbf{b}_1\mathbf{b}_2} E_{\rm R}(C). \end{aligned} \tag{36}$$

Note that, besides this bound, we also have the following unicast bounds for the individual rates

$$R_1\leq \min_{C:\mathbf{a}_1|\mathbf{b}_1} E_{\rm R}(C),\quad R_2\leq \min_{C:\mathbf{a}_2|\mathbf{b}_2} E_{\rm R}(C). \tag{37}$$

These follows directly from the results of Ref. [20, 21] on the converse bounds for unicast quantum networks. Equivalently, we may re-derive these bounds here, by setting $R_2=0$ or $R_1=0$ in the target state of Eq. (24) and repeating the previous derivation. For instance, for $R_2=0$, we have $\phi:=\phi_{\mathbf{a}_1\mathbf{b}_1}^{\otimes nR_1^{\varepsilon,n}}\otimes\sigma_{\mathbf{a}_2\mathbf{b}_2}$, where $\sigma_{\mathbf{a}_2\mathbf{b}_2}$ does not contain target bits and may be taken to be separable. Therefore, we start from $K_{\rm D}(\mathbf{a}_1|\mathbf{b}_1)_{\phi}=nR_1^{\varepsilon,n}$ and repeat the derivation with respect to $\mathbf{a}_1|\mathbf{b}_1$.

It is easy to generalize from $M=2$ to arbitrary M. For any integer M, we have the target state

$$\phi:=\bigotimes_{i=1}^{M}\phi_{\mathbf{a}_i\mathbf{b}_i}^{\otimes nR_i^{\varepsilon,n}}. \tag{38}$$

Considering the bipartition $\{\mathbf{a}_i\}|\{\mathbf{b}_i\}$ and the corresponding cuts of the network leads to

$$\sum_{i=1}^{M}R_i\leq \min_{C:\{\mathbf{a}_i\}|\{\mathbf{b}_i\}} E_{\rm R}(C), \tag{39}$$

where we note that increasing the number of rates reduces the number of possible cuts in the minimization. To get all the remaining inequalities of the theorem, we just need to set some of the rates to zero. For instance, for $R_i\neq 0$ and $R_{j\neq i}=0$, we get the unicast bounds of Eq. (26). For $R_i\neq 0$, $R_{j\neq i}\neq 0$ and $R_{k\neq i,j}=0$ we get the double-unicast bounds of Eq. (27), and so on. The extension to asymptotic simulations of bosonic channels is achieved via the weaker definition of REE in Eq. (9). ■

Once we have Theorem 1, it is immediate to specify the results for the case of multiple-unicast distillable networks, for which we may write $E_{\rm R}(\sigma_{\mathbf{xy}})=E_{\rm R}(\sigma_{\mathcal{E}_{\mathbf{xy}}})=\mathcal{C}_{\mathbf{xy}}$ for each edge $(\mathbf{x},\mathbf{y})\in E$, where $\mathcal{C}_{\mathbf{xy}}$ is the two-way capacity of the associated quantum channel $\mathcal{E}_{\mathbf{xy}}$. In this case, we may directly write

$$E_{\rm R}(C)=\mathcal{C}(C):=\max_{(\mathbf{x},\mathbf{y})\in\tilde{C}}\mathcal{C}_{\mathbf{xy}}, \tag{40}$$

where $\mathcal{C}(C)$ is the single-edge capacity of cut C. Thus, we can express the bounds of Theorem 1 in terms of the capacities of the cuts, immediately proving the following.

Corollary 2 *Consider a multiple-unicast quantum network $\mathcal{N}$ with M sender-receiver pairs $(\mathbf{a}_i,\mathbf{b}_i)$ communicating by means of single-path routing. If the network is*

distillable, then we may write the following outer bounds for the capacity region

$$R_i \leq \min_{C:\mathbf{a}_i|\mathbf{b}_i} \mathcal{C}(C) \quad \textit{for any } i, \tag{41}$$

$$R_i + R_j \leq \min_{C:\mathbf{a}_i\mathbf{a}_j|\mathbf{b}_i\mathbf{b}_j} \mathcal{C}(C) \quad \textit{for any } i \neq j \tag{42}$$

$$\vdots$$

$$\sum_{i=1}^{M} R_i \leq \min_{C:\{\mathbf{a}_i\}|\{\mathbf{b}_i\}} \mathcal{C}(C), \tag{43}$$

where $\mathcal{C}(C)$ is the single-edge capacity of cut C.

Note that we cannot establish the achievability of the outer bounds in Eqs. (41)-(43), apart from the case $M = 1$. This case in fact corresponds to a unicast distillable network for which the bound is achievable by solving the widest path problem [20, 21]. In general, for $M > 1$, achievable lower bounds can be established by combining the point-to-point composition strategies with classical routing algorithms that solve the multiple-version of the widest path problem.

V. MULTIPLE-UNICAST QUANTUM NETWORKS WITH MULTIPATH ROUTING

Here we consider a quantum network where M senders $\{\mathbf{a}_i\}$ and M receivers $\{\mathbf{b}_i\}$ communicate in a pairwise fashion $(\mathbf{a}_i, \mathbf{b}_i)$ by means of multipath routing. In a multipath protocol, the points first agree an orientation for the quantum network. For multiple-unicasts note that both the senders and receivers may assists one with each other as relays of the network. This means that $\{\mathbf{a}_i\}$ are not necessarily sources and $\{\mathbf{b}_i\}$ are not necessarily sinks, i.e., these sets may have both incoming and outgoing edges. Given an orientation, each point multicasts to its out-neighborhood with the assistance of network LOCCs. This flooding process ends when each edge of the network has been exploited. For the next use, the points may agree a different orientation, and so on.

The sequence of the orientations together with the sequence of all network LOCCs (exploited in each orientation) define a multiple-unicast flooding protocol $\mathcal{P}^{\text{flood}}_{\text{M-unicast}}$. Its output will be a shared state $\rho^n_{\{\mathbf{a}_i\}\{\mathbf{b}_i\}}$ which is ε-close to a target state

$$\phi := \bigotimes_{i=1}^{M} \phi_{\mathbf{a}_i\mathbf{b}_i}^{\otimes nR_i^{\varepsilon,n}}, \tag{44}$$

where $\phi_{\mathbf{a}_i\mathbf{b}_i}$ is a one-bit state (private bit or ebit) for the pair $(\mathbf{a}_i, \mathbf{b}_i)$ and $nR_i^{\varepsilon,n}$ the number of its copies. By taking the limit of large n, small ε, and optimizing over $\mathcal{P}^{\text{flood}}_{\text{M-unicast}}$, we define the capacity region associated with the achievable rates $(R^{\text{m}}_1, \ldots, R^{\text{m}}_M)$ for the various quantum tasks. We can then state the following result.

Theorem 3 (Multi-unicast with multipaths) *Let us consider a multiple-unicast quantum network $\mathcal{N} = (P, E)$ with M sender-receiver pairs $(\mathbf{a}_i, \mathbf{b}_i)$ communicating via multipath routing. Adopt a simulation of the network with a resource representation $\sigma(\mathcal{N}) = \{\sigma_{\mathbf{xy}}\}_{(\mathbf{x},\mathbf{y})\in E}$. In particular, $\sigma(\mathcal{N})$ can be a Choi-representation for a teleportation-covariant $\mathcal{N}$. We have the following outer bounds for the capacity region*

$$R_i^m \leq \min_{C:\mathbf{a}_i|\mathbf{b}_i} E^m_{\text{R}}(C) \quad \textit{for any } i, \tag{45}$$

$$R_i^m + R_j^m \leq \min_{C:\mathbf{a}_i\mathbf{a}_j|\mathbf{b}_i\mathbf{b}_j} E^m_{\text{R}}(C) \quad \textit{for any } i \neq j \tag{46}$$

$$\vdots$$

$$\sum_{i=1}^{M} R_i^m \leq \min_{C:\{\mathbf{a}_i\}|\{\mathbf{b}_i\}} E^m_{\text{R}}(C), \tag{47}$$

where $E^m_{\text{R}}(C) := \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\text{R}}(\sigma_{\mathbf{xy}})$ is the multi-edge flow of REE across cut C. It is understood that formulations may be asymptotic for quantum networks with bosonic channels.

Proof. The proof follows the main steps of the one of Theorem 1. As before, consider key generation. For the bipartition $\{\mathbf{a}_i\}|\{\mathbf{b}_i\}$, the distillable key of the target state ϕ is equal to

$$K_{\text{D}}(\{\mathbf{a}_i\}|\{\mathbf{b}_i\})_\phi = n\sum_{i=1}^{M} R_i^{\varepsilon,n} \tag{48}$$

$$\leq E_R(\{\mathbf{a}_i\}|\{\mathbf{b}_i\})_\phi \tag{49}$$

$$\leq E_R(\{\mathbf{a}_i\}|\{\mathbf{b}_i\})_{\rho^n} + \delta(\varepsilon, d), \tag{50}$$

which leads to the inequality

$$\lim_{\varepsilon,n} \sum_{i=1}^{M} R_i^{\varepsilon,n} \leq \lim_{n\to+\infty} n^{-1} E_R(\{\mathbf{a}_i\}|\{\mathbf{b}_i\})_{\rho^n} \ . \tag{51}$$

For any cut $C : \{\mathbf{a}_i\}|\{\mathbf{b}_i\}$ of the (simulated) network, we may write the following decomposition of the output state

$$\rho^n_{\{\mathbf{a}_i\}\{\mathbf{b}_i\}}(C) = \bar{\Lambda}^C_{\{\mathbf{a}_i\}\{\mathbf{b}_i\}} \left[\bigotimes_{(\mathbf{x},\mathbf{y})\in\tilde{C}} \sigma_{\mathbf{xy}}^{\otimes n} \right], \tag{52}$$

for some trace-preserving LOCC $\bar{\Lambda}^C_{\{\mathbf{a}_i\}\{\mathbf{b}_i\}}$. Note that here we have $n_{\mathbf{xy}} = n$. By replacing $\rho^n = \rho^n_{\{\mathbf{a}_i\}\{\mathbf{b}_i\}}(C)$ in Eq. (51), we therefore get

$$\lim_{\varepsilon,n} \sum_{i=1}^{M} R_i^{\varepsilon,n} \leq \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\text{R}}(\sigma_{\mathbf{xy}}) := E^{\text{m}}_{\text{R}}(C). \tag{53}$$

The next step is to minimize over the cuts, leading to

$$\lim_{\varepsilon,n} \sum_{i=1}^{M} R_i^{\varepsilon,n} \leq \min_{C:\{\mathbf{a}_i\}|\{\mathbf{b}_i\}} E^{\text{m}}_{\text{R}}(C). \tag{54}$$

Since the latter inequality holds for any protocol $\mathcal{P}^{\text{flood}}_{\text{M-unicast}}$, it can be extended to the achievable rates

$$\sum_{i=1}^{M} R_i^{\text{m}} = \sup_{\mathcal{P}^{\text{flood}}_{\text{M-unicast}}} \lim_{\varepsilon,n} \sum_{i=1}^{M} R_i^{\varepsilon,n} \leq \min_{C:\{\mathbf{a}_i\}|\{\mathbf{b}_i\}} E_{\text{R}}^{\text{m}}(C). \tag{55}$$

Finally, by setting some of the rates equal to zero in the target state, we may repeat the procedure with respect to different bipartitions and derive all the remaining conditions in Eqs. (45)-(47). The extension to asymptotic simulations of bosonic channels is achieved by adopting the weaker definition of the REE. ■

It is immediate to specify the result for distillable networks for which we may directly write

$$E_{\text{R}}^{\text{m}}(C) = \mathcal{C}^{\text{m}}(C) := \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} \mathcal{C}_{\mathbf{xy}}, \tag{56}$$

where $\mathcal{C}^{\text{m}}(C)$ is the multi-edge capacity of cut C. We may write the following immediate consequence.

Corollary 4 *Consider a multiple-unicast quantum network $\mathcal{N}$ with M sender-receiver pairs $(\mathbf{a}_i, \mathbf{b}_i)$ communicating via multipath routing. If the network is distillable, then we may write the following outer bounds for the capacity region*

$$R_i^m \leq \min_{C:\mathbf{a}_i|\mathbf{b}_i} \mathcal{C}^m(C) \quad \textit{for any } i, \tag{57}$$

$$R_i^m + R_j^m \leq \min_{C:\mathbf{a}_i\mathbf{a}_j|\mathbf{b}_i\mathbf{b}_j} \mathcal{C}^m(C) \quad \textit{for any } i\neq j \tag{58}$$

$$\vdots$$

$$\sum_{i=1}^{M} R_i^m \leq \min_{C:\{\mathbf{a}_i\}|\{\mathbf{b}_i\}} \mathcal{C}^m(C), \tag{59}$$

where $\mathcal{C}^m(C)$ is the multi-edge capacity of cut C.

Achievable lower bounds may be determined by combining the point-to-point composition strategy with classical routing algorithms based on the maximization of multiple flows. For the specific case $M = 1$, the outer bound is achievable and we retrieve the max-flow min-cut theorem for quantum communications [20, 21]. For $M > 2$, achievable lower bounds may be found by exploiting classical literature on multicommodity flow algorithms, e.g., Ref. [51] which showed a version of the max-flow min-cut theorem for undirected networks with two commodities, and Ref. [23] which discusses extensions to more than two commodities.

VI. MULTICAST QUANTUM NETWORKS

Let us now consider a multicast scenario, where Alice $\mathbf{a}$ aims at simultaneously communicate generally-different messages to a set of M receivers, i.e., a set of Bobs $\{\mathbf{b}_i\}$. Because of the implicit parallel nature of this communication process, it is directly formulated under the assumption of multipath routing. We can easily generalize the description of the one-sender one-receiver flooding protocol to the present case of multiple receivers.

In a 1-to-M multicast network protocol, the quantum network $\mathcal{N}$ is subject to an orientation where Alice is treated as a source, while the various Bobs are destination points, each one being a receiver but also a potential relay for another receiver (so that they are not necessarily sinks in the general case). Each end-to-end simultaneous communication between Alice and the Bobs consists of a sequence of multicasts from each point of the network to its out-neighborhood, assisted by network LOCCs. This is done in a flooding fashion so that each edge of the network is exploited. The orientation of the network may be updated and optimized at each round of the protocol.

The sequence of orientations and the network LOCCs define the multicast flooding protocol $\mathcal{P}^{\text{flood}}_{\text{multicast}}$. After n uses of the network, Alice and the M Bobs will share an output state $\rho^n_{\mathbf{a}\{\mathbf{b}_i\}}$ which is ε-close to a target state

$$\phi := \bigotimes_{i=1}^{M} \phi_{\mathbf{ab}_i}^{\otimes nR_i^{\varepsilon,n}}. \tag{60}$$

where $\phi_{\mathbf{ab}_i}$ is a one-bit state (private bit or ebit) for the pair of points $(\mathbf{a}, \mathbf{b}_i)$ and $nR_i^{\varepsilon,n}$ the number of its copies. Note that this is a compact notation which involves countable sets of systems $\mathbf{a} = (a, a', a'', \ldots)$ and $\mathbf{b}_i = (b_i, b_i', b_i'', \ldots)$. Therefore, the tensor product $\phi_{\mathbf{ab}_1}^{\otimes nR_1^{\varepsilon,n}} \otimes \phi_{\mathbf{ab}_2}^{\otimes nR_2^{\varepsilon,n}}$ explicitly means $\phi_{ab_1}^{\otimes nR_1^{\varepsilon,n}} \otimes \phi_{a'b_2'}^{\otimes nR_2^{\varepsilon,n}}$, so that there are different systems involved in Alice's side.

By taking the limit of large n, small ε, and optimizing over $\mathcal{P}^{\text{flood}}_{\text{multicast}}$, we define the capacity region associated with the achievable rates $(R_1, \ldots, R_M)$. In particular, we may define a unique capacity which is associated with the symmetric condition $R_1 = \ldots = R_M$ (or, more precisely, with a guaranteed common rate R with each Bob). In fact, we may consider a symmetric type of protocol $\tilde{\mathcal{P}}^{\text{flood}}_{\text{multicast}}$ whose target state ϕ must have $nR_i^{\varepsilon,n} \geq nR_{\varepsilon,n}$ bits for any i. Then, by taking the asymptotic limit of large n small ε, and maximizing over all such protocols, we may define the multicast network capacity

$$\mathcal{C}^M(\mathcal{N}) = \sup_{\tilde{\mathcal{P}}^{\text{flood}}_{\text{multicast}}} \lim_{\varepsilon,n} R_{\varepsilon,n}. \tag{61}$$

This rate quantifies the maximum number of target bits per network use (multipath transmission) that Alice may simultaneously share with each Bob in the destination set $\{\mathbf{b}_i\}$. We have the usual hierarchy $Q_2^M(\mathcal{N}) = D_2^M(\mathcal{N}) \leq K^M(\mathcal{N})$ when we specify the target state. We can now state the following general bound.

Theorem 5 (Quantum multicast) *Let us consider a multicast quantum network $\mathcal{N}$ with one sender and M receivers $\{\mathbf{b}_i\}$. Adopt a simulation of the network with a resource representation $\sigma(\mathcal{N}) = \{\sigma_{\mathbf{xy}}\}_{(\mathbf{x},\mathbf{y})\in E}$. In*

particular, $\sigma(\mathcal{N})$ can be a Choi-representation for a teleportation-covariant $\mathcal{N}$. Then we have the following outer bounds for the capacity region

$$R_i \leq E_{\mathrm{R}}^{m}(i) := \min_{C:\mathbf{a}|\mathbf{b}_i} E_{\mathrm{R}}^{m}(C) \quad \textit{for any } i, \tag{62}$$

$$R_i + R_j \leq \min_{C:\mathbf{a}|\mathbf{b}_i\mathbf{b}_j} E_{\mathrm{R}}^{m}(C) \quad \textit{for any } i \neq j \tag{63}$$

$$\vdots$$

$$\sum_{i=1}^{M} R_i \leq \min_{C:\mathbf{a}|\{\mathbf{b}_i\}} E_{\mathrm{R}}^{m}(C), \tag{64}$$

where $E_{\mathrm{R}}^{m}(C)$ is the multi-edge flow of REE through cut C. In particular, the multicast network capacity satisfies

$$\mathcal{C}^{M}(\mathcal{N}) \leq \min_{i\in\{1,M\}} E_{\mathrm{R}}^{m}(i). \tag{65}$$

It is understood that formulations may be asymptotic for quantum networks with bosonic channels.

Proof. Consider the upper bound given by secret-key generation. With respect to the bipartition $\mathbf{a}|\{\mathbf{b}_i\}$, we may write the usual steps starting form the distillable key of the target state

$$K_{\mathrm{D}}(\mathbf{a}|\{\mathbf{b}_i\})_{\phi} = n\sum_{i=1}^{M} R_i^{\varepsilon,n} \tag{66}$$

$$\leq E_{\mathrm{R}}(\mathbf{a}|\{\mathbf{b}_i\})_{\phi} \tag{67}$$

$$\leq E_{\mathrm{R}}(\mathbf{a}|\{\mathbf{b}_i\})_{\rho^n} + \delta(\varepsilon, d), \tag{68}$$

leading to the asymptotic limit

$$\lim_{\varepsilon,n}\sum_{i=1}^{M} R_i^{\varepsilon,n} \leq \lim_{n\to+\infty} n^{-1} E_{\mathrm{R}}(\mathbf{a}|\{\mathbf{b}_i\})_{\rho^n}. \tag{69}$$

For any cut $C:\mathbf{a}|\{\mathbf{b}_i\}$ of the (simulated) network, we may write the decomposition

$$\rho^{n}_{\mathbf{a}\{\mathbf{b}_i\}}(C) = \bar{\Lambda}^{C}_{\mathbf{a}\{\mathbf{b}_i\}}\left[\bigotimes_{(\mathbf{x},\mathbf{y})\in\tilde{C}} \sigma_{\mathbf{xy}}^{\otimes n}\right], \tag{70}$$

for some trace-preserving LOCC $\bar{\Lambda}^{C}_{\mathbf{a}\{\mathbf{b}_i\}}$. By replacing $\rho^n = \rho^{n}_{\mathbf{a}\{\mathbf{b}_i\}}(C)$ in Eq. (69), we therefore get

$$\lim_{\varepsilon,n}\sum_{i=1}^{M} R_i^{\varepsilon,n} \leq \sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}} E_{\mathrm{R}}(\sigma_{\mathbf{xy}}) := E_{\mathrm{R}}^{\mathrm{m}}(C). \tag{71}$$

By minimizing over the cuts and maximizing over the protocols, we may write

$$\sum_{i=1}^{M} R_i \leq \min_{C:\mathbf{a}|\{\mathbf{b}_i\}} E_{\mathrm{R}}^{\mathrm{m}}(C). \tag{72}$$

The other conditions in Eqs. (62)-(64) are obtained by setting part of the rates $R_i^{\varepsilon,n}$ to zero in the target state (as in the previous proofs). In particular, set $R_i^{\varepsilon,n} \neq 0$ for some i, while $R_j^{\varepsilon,n} = 0$ for any $j \neq i$. The target state becomes $\phi := \phi_{\mathbf{ab}_i}^{\otimes n R_i^{\varepsilon,n}} \otimes \sigma_{\mathrm{sep}}$ and we repeat the derivation with respect to the bipartition $\mathbf{a}|\mathbf{b}_i$. This leads to

$$\lim_{\varepsilon,n} R_i^{\varepsilon,n} \leq \lim_{n\to+\infty} n^{-1} E_{\mathrm{R}}(\mathbf{a}|\mathbf{b}_i)_{\rho^n}, \tag{73}$$

where we may directly consider the reduced state

$$\rho^n = \rho^{n}_{\mathbf{ab}_i} = \mathrm{Tr}_{\{\mathbf{b}_{j\neq i}\}}\left[\rho^{n}_{\mathbf{a}\{\mathbf{b}_1,\ldots,\mathbf{b}_M\}}\right]. \tag{74}$$

For any cut $C:\mathbf{a}|\mathbf{b}_i$, we therefore have

$$\rho^{n}_{\mathbf{ab}_i}(C) = \bar{\Lambda}^{C}_{\mathbf{ab}_i}\left[\bigotimes_{(\mathbf{x},\mathbf{y})\in\tilde{C}} \sigma_{\mathbf{xy}}^{\otimes n}\right], \tag{75}$$

which leads to $\lim_{\varepsilon,n} R_i^{\varepsilon,n} \leq E_{\mathrm{R}}^{\mathrm{m}}(C)$. By minimizing over the cuts, one gets

$$\lim_{\varepsilon,n} R_i^{\varepsilon,n} \leq E_{\mathrm{R}}^{\mathrm{m}}(i) := \min_{C:\mathbf{a}|\mathbf{b}_i} E_{\mathrm{R}}^{\mathrm{m}}(C). \tag{76}$$

Since this is true for any protocol $\mathcal{P}^M$, it can be extended to the achievable rates, i.e., we get Eq. (62).

For the multicast network capacity, just note that

$$\lim_{\varepsilon,n} R^{\varepsilon,n} \leq \min_i\{\lim_{\varepsilon,n} R_i^{\varepsilon,n}\}. \tag{77}$$

Therefore, from Eq. (76), we may write

$$\lim_{\varepsilon,n} R^{\varepsilon,n} \leq \min_i E_{\mathrm{R}}^{\mathrm{m}}(i). \tag{78}$$

This is true for any symmetric protocol $\mathcal{P}^{M}_{\mathrm{sym}}$ which leads to the result of Eq. (65). Results are extended to asymptotic simulations of bosonic channels in the usual way. ■

As usual, in the case of distillable networks, we may prove stronger results. As a direct consequence of Theorem 5, we may write the following cutset bound.

Corollary 6 *Consider a multicast quantum network $\mathcal{N}$ with one sender and M receivers $\{\mathbf{b}_i\}$. If the network is distillable, then we have the following outer bounds for the capacity region*

$$R_i \leq \mathcal{C}^{m}(i) = \min_{C:\mathbf{a}|\mathbf{b}_i} \mathcal{C}^{m}(C) \quad \textit{for any } i, \tag{79}$$

$$R_i + R_j \leq \min_{C:\mathbf{a}|\mathbf{b}_i\mathbf{b}_j} \mathcal{C}^{m}(C) \quad \textit{for any } i \neq j \tag{80}$$

$$\vdots$$

$$\sum_{i=1}^{M} R_i \leq \min_{C:\mathbf{a}|\{\mathbf{b}_i\}} \mathcal{C}^{m}(C), \tag{81}$$

where $\mathcal{C}^{m}(C)$ is the multi-edge capacity of cut C and $\mathcal{C}^{m}(i)$ is the multipath capacity between the sender and the ith receiver (in a unicast setting). In particular, the multicast network capacity must satisfy the bound

$$\mathcal{C}^{M}(\mathcal{N}) \leq \min_{i\in\{1,M\}} \mathcal{C}^{m}(i)\ . \tag{82}$$

Our previous results refer to the general case of multiple independent messages. In a multicast quantum network, this means that Alice distributes M different sequences of target bits to the M Bobs $\{\mathbf{b}_i\}$. For instance, these may represent M different secret keys, one for each Bob in the destination set. For this specific task (key distribution), the multicast capacity of the network $\mathcal{C}^M(\mathcal{N})$ becomes a multicast secret-key capacity $\mathcal{K}^M(\mathcal{N})$.

In QKD, it is interesting to consider the variant scenario where Alice distributes exactly the same secret key to all Bobs $\{\mathbf{b}_i\}$, e.g., to enable a quantum-secured conference among these parties. For this particular task, we may define a single-key version of the multicast secret-key capacity, that we denote as $\mathcal{K}^M_{\text{1-key}}(\mathcal{N})$. This represents the maximum rate at which Alice may distribute the same secret key to all Bobs in each parallel use of the network. It is clear that we have $\mathcal{K}^M_{\text{1-key}}(\mathcal{N}) \geq \mathcal{K}^M(\mathcal{N})$, just because Alice may use $M-1$ distributed keys to encrypt and share the shortest key with all Bobs.

VII. MULTIPLE-MULTICAST QUANTUM NETWORKS

In the multiple-multicast quantum network, we have M_A Alices $\{\mathbf{a}_1, \ldots, \mathbf{a}_i, \ldots, \mathbf{a}_{M_A}\}$, each of them communicating generally-different messages with a destination set of M_B Bobs $\{\mathbf{b}_1, \ldots, \mathbf{b}_j, \ldots, \mathbf{b}_{M_B}\}$ by means of multipath routing. Each end-to-multiend multicast $\mathbf{a}_i \to \{\mathbf{b}_j\}$ is associated with the distribution of M_B independent sequences of target bits (e.g., secret keys) between the ith Alice $\mathbf{a}_i$ and each Bob $\mathbf{b}_j$ in the destination set. The description of a multiple-multicast protocol for a quantum network follows the same main features discussed for the case of a single-multicast network ($M_A = 1$). Because we have multiple senders and receivers, here we need to consider all possible orientations of the network. Each use of the quantum network is performed under some orientation which is adopted by the points for their out-neighborhood multicasts, suitably assisted by network LOCCs. Use after use, these steps define a multiple-multicast flooding protocol $\mathcal{P}^{\text{flood}}_{\text{M-multicast}}$.

After n uses, the ensembles of Alices and Bobs share an output state $\rho^n_{\{\mathbf{a}_i\}\{\mathbf{b}_j\}}$ which is ε-close to a target state

$$\phi := \bigotimes_{i=1}^{M_A} \bigotimes_{j=1}^{M_B} \phi_{\mathbf{a}_i\mathbf{b}_j}^{\otimes n R^{\varepsilon,n}_{ij}}. \tag{83}$$

where $\phi_{\mathbf{a}_i\mathbf{b}_j}$ is a one-bit state (private bit or ebit) for the pair $(\mathbf{a}_i, \mathbf{b}_j)$ and $nR^{\varepsilon,n}_{ij}$ the number of its copies. By taking the limit of large n, small ε, and optimizing over $\mathcal{P}^{\text{flood}}_{\text{M-multicast}}$, we define the capacity region for the achievable rates $\{R_{ij}\}$. Assume the symmetric case where the ith Alice $\mathbf{a}_i$ achieves the same rate $R_{i1} = \ldots = R_{iM_B}$ with all Bobs $\{\mathbf{b}_j\}$ (or, more precisely, a guaranteed common rate R_i). This means to consider symmetric protocols whose target state ϕ must have $\min_j R^{\varepsilon,n}_{ij} \geq R^{\varepsilon,n}_i$ bits for any i. By taking the asymptotic limit of $R^{\varepsilon,n}_i$ for large n, small ε, and maximizing over all these symmetric protocols, we may define the capacity region for the achievable multicast rates $(R_1, \ldots, R_{M_A})$. In the latter set, rate R_i provides the minimum number of target bits per use that the ith Alice may share with each Bob in the destination set $\{\mathbf{b}_j\}$ (in the multi-message setting, i.e., assuming independent sequences shared with the various Bobs). We have the following outer bounds to the capacity region.

Theorem 7 (Quantum multiple-multicast) *Let us consider a multiple-multicast quantum network $\mathcal{N} = (P, E)$ where each of the M_A senders $\{\mathbf{a}_i\}$ communicates with M_B receivers $\{\mathbf{b}_j\}$ at the multicast rate R_i. Adopt a simulation of $\mathcal{N}$ with some resource representation $\sigma(\mathcal{N}) = \{\sigma_{\mathbf{xy}}\}_{(\mathbf{x},\mathbf{y})\in E}$, which may be a Choi-representation for a teleportation-covariant $\mathcal{N}$. Then, we have the following outer bounds for the capacity region*

$$R_i \leq \min_{\substack{C:\mathbf{a}_i\in\mathbf{A}\\ \{\mathbf{b}_j\}\cap\mathbf{B}\neq\emptyset}} E^m_{\text{R}}(C), \tag{84}$$

$$R_i + R_j \leq \min_{\substack{C:\mathbf{a}_i,\mathbf{a}_j\in\mathbf{A}\\ \{\mathbf{b}_j\}\cap\mathbf{B}\neq\emptyset}} E^m_{\text{R}}(C), \tag{85}$$

$$\vdots$$

$$\sum_{i=1}^{M_A} R_i \leq \min_{\substack{C:\{\mathbf{a}_i\}\subseteq\mathbf{A}\\ \{\mathbf{b}_j\}\cap\mathbf{B}\neq\emptyset}} E^m_{\text{R}}(C), \tag{86}$$

where $E^m_{\text{R}}(C)$ is the multi-edge flow of REE through cut C. For a distillable network, we may write the bounds in Eqs. (84)-(86) with $E^m_{\text{R}}(C) = \mathcal{C}^m(C)$, i.e., in terms of the multi-edge capacity of the cuts.

Proof. Consider the upper bound given by secret-key generation. With respect to the bipartition $\{\mathbf{a}_i\}|\{\mathbf{b}_j\}$, we can manipulate the distillable key K_{D} of the target state ϕ as follows

$$K_{\text{D}}(\{\mathbf{a}_i\}|\{\mathbf{b}_j\})_\phi = n \sum_{i=1}^{M_A}\sum_{j=1}^{M_B} R^{\varepsilon,n}_{ij} \tag{87}$$

$$\leq E_{\text{R}}(\{\mathbf{a}_i\}|\{\mathbf{b}_j\})_\phi \tag{88}$$

$$\leq E_{\text{R}}(\{\mathbf{a}_i\}|\{\mathbf{b}_j\})_{\rho^n} + \delta(\varepsilon, d), \tag{89}$$

leading to the asymptotic limit

$$\lim_{\varepsilon,n} \sum_{i=1}^{M_A}\sum_{j=1}^{M_B} R^{\varepsilon,n}_{ij} \leq \lim_{n\to+\infty} n^{-1} E_{\text{R}}(\{\mathbf{a}_i\}|\{\mathbf{b}_j\})_{\rho^n}. \tag{90}$$

For any cut $C : \{\mathbf{a}_i\}|\{\mathbf{b}_j\}$ of the (simulated) network, we may write the decomposition

$$\rho^n_{\{\mathbf{a}_i\}\{\mathbf{b}_j\}}(C) = \bar{\Lambda}^C_{\{\mathbf{a}_i\}\{\mathbf{b}_j\}}\left[\bigotimes_{(\mathbf{x},\mathbf{y})\in\tilde{C}} \sigma^{\otimes n}_{\mathbf{xy}}\right], \tag{91}$$

and manipulate Eq. (90) into the following

$$\lim_{\varepsilon,n}\sum_{i=1}^{M_A}\sum_{j=1}^{M_B}R_{ij}^{\varepsilon,n}\leq\sum_{(\mathbf{x},\mathbf{y})\in\tilde{C}}E_{\mathrm{R}}(\sigma_{\mathbf{xy}}):=E_{\mathrm{R}}^{\mathrm{m}}(C). \quad (92)$$

By minimizing over the cuts and maximizing over the protocols, we may write

$$\sum_{i=1}^{M_A}\sum_{j=1}^{M_B}R_{ij}\leq\min_{C:\{\mathbf{a}_i\}|\{\mathbf{b}_j\}}E_{\mathrm{R}}^{\mathrm{m}}(C)\ . \quad (93)$$

By setting part of the rates $R_{ij}^{\varepsilon,n}$ to zero in the target state, we derive the full set of conditions

$$\sum_{i=1}^{M_A}\sum_{j=1}^{M_B}R_{ij}\leq\min_{C:\{\mathbf{a}_i\}|\{\mathbf{b}_j\}}E_{\mathrm{R}}^{\mathrm{m}}(C), \quad (94)$$

$$\vdots$$

$$R_{ij}+R_{kl}\leq\min_{C:\mathbf{a}_i\mathbf{a}_k|\mathbf{b}_j\mathbf{b}_l}E_{\mathrm{R}}^{\mathrm{m}}(C), \quad (95)$$

$$R_{ij}\leq\min_{C:\mathbf{a}_i|\mathbf{b}_j}E_{\mathrm{R}}^{\mathrm{m}}(C). \quad (96)$$

The latter conditions are valid for the end-to-end rates R_{ij} achievable between each pair $(\mathbf{a}_i,\mathbf{b}_j)$. We are interested in the achievable multicast rates $\{R_i\}$ between each sender $\mathbf{a}_i$ and all receivers $\{\mathbf{b}_j\}$. Corresponding conditions can be derived by considering a subset of protocols with target state of the type

$$\phi_k:=\bigotimes_{i=1}^{M_A}\phi_{\mathbf{a}_i\mathbf{b}_k}^{\otimes nR_{ik}^{\varepsilon,n}}\otimes\sigma_{\mathrm{sep}}, \quad (97)$$

for some k, where all Alices $\{\mathbf{a}_i\}$ aim to optimize their rates $\{R_{ik}^{\varepsilon,n}\}$ with some fixed Bob $\mathbf{b}_k$, so that $R_{ij}^{\varepsilon,n}=0$ for any $j\neq k$. By repeating the previous steps with respect to the bipartition $\{\mathbf{a}_i\}|\mathbf{b}_k$, we obtain

$$\lim_{\varepsilon,n}\sum_{i=1}^{M_A}R_{ik}^{\varepsilon,n}\leq\min_{C:\{\mathbf{a}_i\}|\mathbf{b}_k}E_{\mathrm{R}}^{\mathrm{m}}(C). \quad (98)$$

Since we have $R_i^{\varepsilon,n}\leq\min_j R_{ij}^{\varepsilon,n}\leq R_{ik}^{\varepsilon,n}$ for any i, we can then write the same inequality for $\lim_{\varepsilon,n}\sum_{i=1}^{M_A}R_i^{\varepsilon,n}$. Then, by optimizing over the protocols, we get

$$\sum_{i=1}^{M_A}R_i\leq\min_{C:\{\mathbf{a}_i\}|\mathbf{b}_k}E_{\mathrm{R}}^{\mathrm{m}}(C). \quad (99)$$

Because we may repeat the previous reasoning for any k, we may write

$$\sum_{i=1}^{M_A}R_i\leq\min_{C}E_{\mathrm{R}}^{\mathrm{m}}(C), \quad (100)$$

with $C=(\mathbf{A},\mathbf{B})$ such that $\{\mathbf{a}_i\}\subseteq\mathbf{A}$ and $\{\mathbf{b}_j\}\cap\mathbf{B}\neq\emptyset$.

Now, for any fixed k, impose that the rates $\{R_{ik}^{\varepsilon,n}\}$ are zero for some of the Alices $\{\mathbf{a}_i\}$. If we set $R_{ik}^{\varepsilon,n}\neq 0$ for a pair $(\mathbf{a}_i,\mathbf{b}_k)$, then the condition $R_i^{\varepsilon,n}\leq R_{ik}^{\varepsilon,n}$ leads to

$$R_i\leq\min_{C:\mathbf{a}_i|\mathbf{b}_k}E_{\mathrm{R}}^{\mathrm{m}}(C). \quad (101)$$

Because the reasoning can be repeated for any k, we may then write

$$R_i\leq\min_{C}E_{\mathrm{R}}^{\mathrm{m}}(C), \quad (102)$$

with $C=(\mathbf{A},\mathbf{B})$ such that $\mathbf{a}_i\in\mathbf{A}$ and $\{\mathbf{b}_j\}\cap\mathbf{B}\neq\emptyset$. Extending the previous reasoning to two non-zero rates $R_{ik}^{\varepsilon,n}\neq 0$ and $R_{jk}^{\varepsilon,n}\neq 0$ leads to

$$R_i+R_j\leq\min_{C}E_{\mathrm{R}}^{\mathrm{m}}(C), \quad (103)$$

with $C=(\mathbf{A},\mathbf{B})$ such that $\mathbf{a}_i,\mathbf{a}_j\in\mathbf{A}$ and $\{\mathbf{b}_j\}\cap\mathbf{B}\neq\emptyset$. Other similar conditions can be derived for the multicast rates, so that we get the result of Eqs. (84)-(86). Finally, for a distillable network we have $E_{\mathrm{R}}^{\mathrm{m}}(C)=\mathcal{C}^{\mathrm{m}}(C)$ and, therefore, it is immediate to express these results in terms of the multi-edge capacities of the cuts. ■

VIII. CONCLUSIONS

In this information-theoretic work, we have investigated the ultimate rates for transmitting quantum information, distributing entanglement and generating secret keys between multiple senders and receivers in an arbitrary quantum network, assuming single- or multi-path routing strategies. We have established general single-letter REE upper bounds for the various multi-end capacities associated to the various configurations of multiple-unicast, multicast, and multiple-multicast quantum networks. The bounds apply to networks connected by arbitrary quantum channels (at any dimension) with more specific formulations in the case of teleportation-covariant and distillable channels. In particular, the case of quantum networks connected by bosonic channels is implicitly treated by using asymptotic LOCC simulations, so that the results are automatically proven for fundamental noise models at the optical and telecom regimes, such as the pure-loss channels.

The present paper provides a multiend generalization of the results of Ref. [20] (first appeared in Ref. [21]) for the basic end-to-end (unicast) scenario. It also extends the results presented in Ref. [52] from single-hop to multi-hop quantum networks. Due to the much more complex scenarios associated with the simultaneous multi-hop quantum communication among multiple senders and receivers, we could only bound the capacity regions in the various configurations analyzed, so that their full characterization remains an open question for further investigations.

Acknowledgments. This work has been supported by the EPSRC via the 'UK Quantum Communications

HUB' (EP/M013472/1) and by the European Union via the project 'Continuous Variable Quantum Communications' (CiViQ, no 820466).

[1] M. A. Nielsen, and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).

[2] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[3] A. Holevo, *Quantum Systems, Channels, Information: A Mathematical Introduction* (De Gruyter, Berlin-Boston, 2012).

[4] C. Weedbrook *et al.*, Rev. Mod. Phys. **84**, 621 (2012).

[5] J. Watrous, *The theory of quantum information* (Cambridge University Press, Cambridge, 2018).

[6] C. H. Bennett and G. Brassard, Proc. IEEE International Conf. on Computers, Systems, and Signal Processing, Bangalaore, pp. 175–179 (1984).

[7] A. K. Ekert, Phys. Rev. Lett. **67**, 661-663 (1991).

[8] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunan-dar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography", preprint arXiv:1906.01645 (2019).

[9] H. J. Kimble, Nature **453**, 1023-1030 (2008).

[10] S. Pirandola, and S. L. Braunstein, Nature **532**, 169-171 (2016).

[11] S. Wehner, D. Elkouss, and R. Hanson, Science **362**, 303 (2018).

[12] R. Van Meter, *Quantum Networking* (Wiley, 2014).

[13] S. Pirandola, R. Laurenza, C. Ottaviani and L. Banchi, Nat. Commun. **8**, 15043 (2017). See also arXiv:1510.08863 (2015).

[14] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **102**, 050503 (2009).

[15] R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, Phys. Rev. Lett. **102**, 210501 (2009).

[16] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) **557**, 400-403 (2018).

[17] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932-5935 (1998).

[18] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).

[19] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).

[20] S. Pirandola, *End-to-end capacities of a quantum communication network*, Commun. Phys. **2**, 51 (2019).

[21] S. Pirandola, *Capacities of repeater-assisted quantum communications*, arXiv:1601.00966 (2016).

[22] P. Slepian, *Mathematical Foundations of Network Analysis* (Springer-Verlag, New York, 1968).

[23] A. Schrijver, *Combinatorial Optimization* (Springer-Verlag, Berlin, 2003).

[24] A. El Gamal and Y.-H. Kim, *Network Information Theory*, (Cambridge Univ. Press, 2011).

[25] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, (Wiley, New Jersey, 2006).

[26] R. K. Ahuja, T. L. Magnanti, and J. B. Orlin, *Network Flows: Theory, Algorithms and Applications* (Prentice Hall, 1993).

[27] S. Pirandola, and C. Lupo, Phys. Rev. Lett. **118**, 100502 (2017).

[28] T. P. W. Cope, L. Hetzel, L. Banchi, and S. Pirandola, Phys. Rev. A **96**, 022323 (2017).

[29] S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, and L. Banchi, Quant. Sci. Tech. **3**, 035009 (2018).

[30] S. Pirandola, R. Laurenza, and S. L. Braunstein, Eur. Phys. J. D **72**, 162 (2018).

[31] R. Laurenza, C. Lupo, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Quantum Meas. Quantum Metrol. **5**, 1-12 (2018).

[32] S. Pirandola, B. Roy Bardhan, T. Gehring, C. Weedbrook, and S. Lloyd, Nat. Photon. **12**, 724-733 (2018).

[33] V. Vedral, Rev. Mod. Phys. **74**, 197 (2002).

[34] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275-2279 (1997).

[35] V. Vedral, and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

[36] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).

[37] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895-1899 (1993).

[38] S. L. Braunstein, and H. J. Kimble, Phys. Rev. Lett. **80**, 869–872 (1998).

[39] S. L. Braunstein, G. M. D'Ariano, G. J. Milburn, and M. F. Sacchi, Phys. Rev. Lett. **84**, 3486–3489 (2000).

[40] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, Nature Photon. **9**, 641-652 (2015).

[41] M. Christiandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, Lecture Notes in Computer Science **4392**, 456-478 (2007). See also arXiv:quant-ph/0608199v3 for a more extended version.

[42] M. Christiandl, N. Schuch, and A. Winter, Comm. Math. Phys. **311**, 397-422 (2012).

[43] B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).

[44] S. Lloyd, Phys. Rev. A **55,** 1613 (1997).

[45] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks* (5th Edition, Pearson, 2010).

[46] T. E. Harris, and F. S. Ross, Research Memorandum, Rand Corporation (1955).

[47] L. R. Ford, and D. R. Fulkerson, Canadian Journal of Mathematics **8**, 399 (1956).

[48] P. Elias, A. Feinstein, and C. E. Shannon, IRE Trans. Inf. Theory **2**, 117–119 (1956).

[49] J. Edmonds and R. M. Karp, Journal of the ACM **19**, 248–264 (1972).

[50] E. A. Dinic, Soviet Math. Doklady (Doklady) **11**, 1277–1280 (1970).

[51] T. C. Hu, Oper. Res. **11**, 344-360 (1963).

[52] R. Laurenza, and S. Pirandola, Phys. Rev. A **96**, 032318 (2017).